PATENT
81942.0013
Express Mail Label No. EL 713 623 286 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Yasuyuki MURAKAMI et al.

Serial No: Not assigned

Filed: January 23, 2001

For: SECRET KEY GENERATING METHOD, COMMON KEY GENERATING METHOD, ENCRYPTION METHOD, CRYPTOGRAPHIC COMMUNICATION METHOD AND CRYPTOGRAPHIC COMMUNICATION SYSTEM

Art Unit: Not assigned

Examiner: Not assigned

TRANSMITTAL OF PRIORITY DOCUMENT

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2000-016354 which was filed January 25, 2000, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: January 23, 2001

By: _____

Louis A. Mok
Registration No. 22,585
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

日　本　国　特　許　庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:　２０００年　１月２５日

出願番号
Application Number:　特願２０００－０１６３５４

出願人
Applicant (s):　村田機械株式会社
笠原　正雄
辻井　重男

２０００年　８月１８日

特許庁長官
Commissioner,
Patent Office　及川耕造

出証番号　出証特２０００－３０６４８４０

【書類名】　特許願

【整理番号】　20871

【提出日】　平成12年 1月25日

【あて先】　特許庁長官殿

【国際特許分類】　G09C 1/00

H04L 9/00

【発明の名称】　秘密鍵生成方法

【請求項の数】　3

【発明者】

【住所又は居所】　京都府京都市伏見区竹田向代町１３６番地　村田機械株式会社　本社工場内

【氏名】　村上　恭通

【発明者】

【住所又は居所】　大阪府箕面市粟生外院４丁目１５番３号

【氏名】　笠原　正雄

【発明者】

【住所又は居所】　東京都渋谷区神宮前四丁目２番１９号

【氏名】　辻井　重男

【特許出願人】

【識別番号】　000006297

【氏名又は名称】　村田機械株式会社

【代表者】　村田　純一

【特許出願人】

【識別番号】　597008636

【氏名又は名称】　笠原　正雄

【特許出願人】

【識別番号】　598159964

【氏名又は名称】　辻井　重男

出証特２０００－３０６４８４０

【復代理人】

【識別番号】　100114557

【弁理士】

【氏名又は名称】　河野　英仁

【電話番号】　06-6944-4141

【代理人】

【識別番号】　100078868

【弁理士】

【氏名又は名称】　河野　登夫

【電話番号】　06-6944-4141

【手数料の表示】

【予納台帳番号】　001889

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9805283

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　秘密鍵生成方法

【特許請求の範囲】

【請求項１】　複数のセンタの夫々にて、エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎の秘密の対称行列とを用いて、前記エンティティ固有の秘密鍵を生成する方法において、前記各分割特定情報に応じて前記対称行列の一部の成分を取り出し、取り出した成分に前記エンティティ固有の乱数を合成することにより、前記エンティティ固有の秘密鍵を生成することを特徴とする秘密鍵生成方法。

【請求項２】　一のセンタ自身で生成したハッシュ関数と他のセンタで生成されたハッシュ関数とに基づいて、前記一のセンタでの前記乱数を生成する請求項１に記載の秘密鍵生成方法。

【請求項３】　複数のセンタの夫々にて、エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎の秘密の対称行列とを用いて、前記エンティティ固有の秘密鍵を生成する方法において、前記各分割特定情報に応じて前記対称行列の一部の成分を取り出し、前記各分割特定情報に応じて各センタ固有のマスクパターンを生成し、取り出した成分を前記マスクパターンでマスクすることにより、前記エンティティ固有の秘密鍵を生成することを特徴とする秘密鍵生成方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、暗号通信システムのセンタにて各エンティティ固有の秘密鍵を生成する秘密鍵生成方法に関する。

【０００２】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオ

リジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事，外交面で用いられてきた暗号技術が注目されている。

【０００３】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【０００４】

暗号化鍵と復号鍵とは、等しくても良いし、異なっていても良い。両者の鍵が等しい暗号系は、共通鍵暗号系と呼ばれ、米国商務省標準局が採用したＤＥＳ（Data Encryption Standards)はその典型例である。また、両者の鍵が異なる暗号系の一例として、公開鍵暗号系と呼ばれる暗号系が提案された。この公開鍵暗号系は、暗号系を利用する各ユーザ（エンティティ）が暗号化鍵と復号鍵とを一対ずつ作成し、暗号化鍵を公開鍵リストにて公開し、復号鍵のみを秘密に保持するという暗号系である。公開鍵暗号系では、この一対となる暗号化鍵と復号鍵とが異なり、一方向性関数を利用することによって暗号化鍵から復号鍵を割り出せないという特徴を持たせている。

【０００５】

公開鍵暗号系は、暗号化鍵を公開するという画期的な暗号系であって、高度情報化社会の確立に必要な上述した３つの要素に適合するものであり、情報通信技術の分野等での利用を図るべく、その研究が活発に行われ、典型的な公開鍵暗号

系としてＲＳＡ暗号系が提案された。このＲＳＡ暗号系は、一方向性関数として素因数分解の困難さを利用して実現されている。また、離散対数問題を解くことの困難さ（離散対数問題）を利用した公開鍵暗号系も種々の手法が提案されてきた。

【０００６】

また、各エンティティの住所，氏名等の個人を特定するＩＤ（Identity）情報を利用する暗号系が提案された。この暗号系では、ＩＤ情報に基づいて送受信者間で共通の暗号化鍵を生成する。また、このＩＤ情報に基づく暗号技法には、（１）暗号文通信に先立って送受信者間での予備通信を必要とする方式と、（２）暗号文通信に先立って送受信者間での予備通信を必要としない方式とがある。特に、（２）の手法は予備通信が不要であるので、エンティティの利便性が高く、将来の暗号系の中枢をなすものと考えられている。

【０００７】

この（２）の手法による暗号系は、ＩＤ－ＮＩＫＳ（ID-based non-interactive key sharing scheme)と呼ばれており、通信相手のＩＤ情報を用いて予備通信を行うことなく暗号化鍵を共有する方式を採用している。ＩＤ－ＮＩＫＳは、送受信者間で公開鍵，秘密鍵を交換する必要がなく、また鍵のリスト及び第三者によるサービスも必要としない方式であり、任意のエンティティ間で安全に通信を行える。

【０００８】

図５は、このＩＤ－ＮＩＫＳのシステムの原理を示す図である。信頼できるセンタの存在を仮定し、このセンタを中心にして共通鍵生成システムを構成している。図５において、エンティティＸの特定情報であるエンティティＸの名前，住所，電話番号等のＩＤ情報は、ハッシュ関数ｈ（・）を用いてｈ（ID_X）で表す。センタは任意のエンティティＸに対して、センタ公開情報｛PC_i｝，センタ秘密情報｛SC_i｝及びエンティティＸのＩＤ情報ｈ（ID_X）に基づいて、以下のように秘密情報S_{Xi}を計算し、秘密裏にエンティティＸへ配布する。

$$S_{Xi}=F_i\ (\{SC_i\},\ \{PC_i\},\ h(ID_X))$$

【０００９】

エンティティＸは他の任意のエンティティＹとの間で、暗号化，復号のための共通鍵K_{XY}を、エンティティＸ自身の秘密情報｛S_{Xi}｝，センタ公開情報｛PC_i｝及び相手先のエンティティＹのＩＤ情報ｈ（ID_Y）を用いて以下のように生成する。

$$K_{XY}=f(\{S_{Xi}\},\{PC_i\},h(ID_Y))$$

また、エンティティＹも同様にエンティティＸへの鍵を共通鍵K_{YX}を生成する。もし常に$K_{XY}=K_{YX}$の関係が成立すれば、この鍵K_{XY}，K_{YX}をエンティティＸ，Ｙ間で暗号化鍵，復号鍵として使用できる。

【００１０】

上述した公開鍵暗号系では、例えばＲＳＡ暗号系の場合にその公開鍵の長さは現在の電話番号の十数倍となり、極めて煩雑である。これに対して、ＩＤ－ＮＩＫＳでは、各ＩＤ情報を名簿という形式で登録しておけば、この名簿を参照して任意のエンティティとの間で共通鍵を生成することができる。従って、図５に示すようなＩＤ－ＮＩＫＳのシステムが安全に実現されれば、多数のエンティティが加入するコンピュータネットワーク上で便利な暗号系を構築できる。このような理由により、ＩＤ－ＮＩＫＳが将来の暗号系の中心になると期待されている。

【００１１】

このＩＤ－ＮＩＫＳには、次のような２つの問題点がある。一つは、センタがBig Brother となる（すべてのエンティティの秘密を握っており、Key Escrow System になってしまう）点である。もう一つは、ある数のエンティティが結託するとセンタの秘密を演算できる可能性がある点である。この結託問題については、これを計算量的に回避するための工夫が多数なされているが、完全な解決は困難である。

【００１２】

この結託問題の難しさは、特定情報（ＩＤ情報）に基づく秘密パラメータがセンタ秘密と個人秘密との二重構造になっていることに起因する。ＩＤ－ＮＩＫＳでは、センタの公開パラメータと個人の公開された特定情報（ＩＤ情報）とこの２種類の秘密パラメータとにて暗号系が構成され、しかも各エンティティが各自に配布された個人秘密を見せ合ってもセンタ秘密が露呈されないようにする必要

がある。よって、その暗号系の構築の実現には解決すべき課題が多い。

【００１３】

そこで、本発明者等は、特定情報（ＩＤ情報）をいくつかに分割し、複数のセンタの夫々からその分割した特定情報（ＩＤ情報）に基づくすべての秘密鍵をエンティティに配布することにより、数学的構造を最小限に抑えることができて、結託問題の回避を可能にし、その暗号系の構築が容易であるＩＤ－ＮＩＫＳによる暗号手法（以下、これを先行例という）を提案している。

【００１４】

結託問題を解決することを目的として提案されてきたエンティティの特定情報（ＩＤ情報）に基づく種々の暗号系が不成功となった理由は、エンティティの結託情報からセンタ秘密を割り出せないようにするための工夫を数学的構造に求め過ぎていたためである。数学的構造が複雑過ぎると、安全性を証明するための方法も困難となる。そこで、先行例の提案方法では、エンティティの特定情報（ＩＤ情報）をいくつかに分割し、分割した各特定情報（ＩＤ情報）についてすべての秘密鍵をエンティティに配布することにより、数学的構造を最小限に抑えるようにする。

【００１５】

先行例では、信頼される複数のセンタが設けられ、各センタは各エンティティの分割した各特定情報（ＩＤ情報）に対応する数学的構造を持たない秘密鍵を夫々生成して、各エンティティへ送付する。各エンティティは、各センタから送られてきたこれらの秘密鍵と通信相手の公開されている特定情報（ＩＤ情報）とから共通鍵を、予備通信を行わずに生成する。これらの各秘密鍵に含まれている通信相手に対応する成分を夫々取り出し、取り出した成分を合成加算して共通鍵を生成する。よって、すべてのエンティティの秘密を１つのセンタが握るようなことはなく、各センタがBig Brother にならない。

【００１６】

以下、この先行例の概要を説明する。各エンティティの氏名，住所などを示す特定情報であるＩＤベクトルをＬ次元２進ベクトルとし、そのＩＤベクトルをブロックサイズＭ毎にＪ個のブロックに分割する。例えば、エンティティＸのＩＤ

ベクトル（ベクトルI_X）を下記（１）のように分割する。分割特定情報である各ベクトルI_{Xj}（ｊ＝１，２，・・・，Ｊ）をＩＤ分割ベクトルと呼ぶ。なお、各エンティティの公開ＩＤベクトルはハッシュ関数により、Ｌ（＝ＭＪ）ビットに変換される。また、ＩＤベクトルの分割数に応じてＪ個のセンタを設置し、ｊ＝１，２，・・・，Ｊをセンタ番号とする。

【００１７】

【数１】

$$\overrightarrow{I_X} = [\overrightarrow{I_{X1}} \mid \overrightarrow{I_{X2}} \mid \cdots \mid \overrightarrow{I_{XJ}}] \quad \cdots(1)$$

【００１８】

ｊ番目のセンタは、ランダムな数を要素とする対称行列H_j（$2^M \times 2^M$）を作成する。但し、共通鍵のサイズをＳとして、下記（２）～（４）とする。

【００１９】

【数２】

$$H_j = (k_{ab}^{(j)}) \quad \cdots(2)$$

$$k_{ab}^{(j)} \in Z_{2^S} \quad \cdots(3)$$

$$a, b \in Z_{2^M} \quad \cdots(4)$$

【００２０】

また、ｊ番目のセンタは、各エンティティに対して、対称行列H_jより、そのエンティティのＩＤ分割ベクトルに対応する行ベクトルを秘密配布する。即ち、エンティティＸに対しては、ベクトル$s_{Xj}=H_j$〔ベクトルI_{Xj}〕を配布する。このH_j〔ベクトルI_{Xj}〕は、対称行列H_jよりベクトルI_{Xj}に対応した行を１行抜き出したベクトルを表す。各エンティティに配布されたパラメータを秘密ベクトルと呼ぶ。

【００２１】

エンティティＸ，Ｙ間で共通鍵を共有するとする。エンティティＸは、各セン

タから受け取ったっ各秘密ベクトルから、エンティティＹに対応する成分を取り出し、これらのＪ個の成分を合成することにより、エンティティＹに対する共通鍵を生成する。エンティティＹも、エンティティＸに対する共通鍵を同様に生成する。各センタでが生成する秘密行列H_jの対称性によって、エンティティＸ，Ｙは同一の共通鍵を共有できる。このようにして生成した共通鍵を用いて、エンティティＸ，Ｙ間での暗号化処理・復号処理を行う。

【００２２】

【発明が解決しようとする課題】

本発明者等は、このような先行例の改良を研究しており、その先行例を適用した暗号通信システムの構築を図っている。この先行例は、非常に高速に共通鍵を共有できるという優れた長所を有する。しかしながら、各エンティティにとって、全体のＩＤベクトルが一致することは考えられないが、その一部であるＩＤ分割ベクトルが同一となることは考えられる。よって、複数のエンティティが結託して、自身の秘密の部分鍵を提供することにより、各エンティティのＩＤ分割ベクトルの合成にてその全体のＩＤベクトルが構成される他のエンティティになりすますという結託攻撃に弱いという難点があり、更なる改善が望まれている。このような難点は、各センタの秘密の対称行列の一部をそのままエンティティへ配布していることに起因する。

【００２３】

本発明は斯かる事情に鑑みてなされたものであり、先行例と同様に鍵共有の高速性は維持しながら、先行例と比べて安全性を向上できる秘密鍵生成方法を提供することを目的とする。

【００２４】

【課題を解決するための手段】

請求項１に係る秘密鍵生成方法は、複数のセンタの夫々にて、エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎の秘密の対称行列とを用いて、前記エンティティ固有の秘密鍵を生成する方法において、前記各分割特定情報に応じて前記対称行列の一部の成分を取り出し、取り出した成分に前記エンティティ固有の乱数を合成することにより、前記エンティティ固有の

秘密鍵を生成することを特徴とする。

【００２５】

請求項２に係る秘密鍵生成方法は、請求項１において、一のセンタ自身で生成したハッシュ関数と他のセンタで生成されたハッシュ関数とに基づいて、前記一のセンタでの前記乱数を生成することを特徴とする。

【００２６】

請求項３に係る秘密鍵生成方法は、複数のセンタの夫々にて、エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎の秘密の対称行列とを用いて、前記エンティティ固有の秘密鍵を生成する方法において、前記各分割特定情報に応じて前記対称行列の一部の成分を取り出し、前記各分割特定情報に応じて各センタ固有のマスクパターンを生成し、取り出した成分を前記マスクパターンでマスクすることにより、前記エンティティ固有の秘密鍵を生成することを特徴とする。

【００２７】

第１発明では、エンティティの各分割特定情報（ＩＤ分割ベクトル）に応じて対称行列の一部の成分を取り出し、取り出した成分に各エンティティ固有の乱数を合成して、各エンティティ固有の秘密鍵を生成する。よって、個人乱数を加えるので、センタの秘密が露呈されず、安全性が向上する。

【００２８】

第２発明では、第１発明において、自身で生成したハッシュ関数と他のセンタで生成されたハッシュ関数とを用いて、取り出した成分に合成すべき乱数を生成する。よって、全てのセンタが対等となり、ある特定のセンタがBig Brother となることを防止できる。

【００２９】

第３発明では、エンティティの各分割特定情報（ＩＤ分割ベクトル）に応じて対称行列の一部の成分を取り出し、その分割特定情報（ＩＤ分割ベクトル）に基づいて各センタ固有のマスクパターンを生成し、取り出した成分をそのマスクパターンでマスクして、各エンティティ固有の秘密鍵を生成する。よって、両エンティティにおいて分割特定情報（ＩＤ分割ベクトル）が同じであっても、そのマ

スクパターンは異なり、結託攻撃に強くなる。

【００３０】

第１発明及び第３発明の特徴を併せた手法にて各エンティティ固有の秘密鍵を生成する場合には、乱数置換攻撃が成立しない。

【００３１】

また、本発明では、共通鍵を生成する際に各センタからの成分をＸＯＲ合成しており、桁上がりの問題を解消している。

【００３２】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図１は、本発明の暗号通信システムの構成を示す模式図である。情報の隠匿を信頼できる複数（Ｊ個）のセンタ１が設定されており、これらのセンタ１としては、例えば社会の公的機関を該当できる。

【００３３】

これらの各センタ１と、この暗号通信システムを利用するユーザとしての複数の各エンティティａ，ｂ，…，ｚとは、通信路2_{a1}，…，2_{aJ}、2_{b1}，…，2_{bJ}、・・・、2_{z1}，…，2_{zJ}により接続されており、これらの通信路を介して、各センタ１から各エンティティ固有の秘密鍵（秘密ベクトル）が各エンティティａ，ｂ，…，ｚへ伝送されるようになっている。また、２人のエンティティの間には通信路３ab，３az，３bz，…が設けられており、この通信路３ab，３az，３bz，…を介して通信情報を暗号化した暗号文が互いのエンティティ間で伝送されるようになっている。

【００３４】

図２は、２人のエンティティａ，ｂ間における情報の通信状態を示す模式図である。図２の例は、エンティティａが平文（メッセージ）Ｍを暗号文Ｃに暗号化してそれをエンティティｂへ送信し、エンティティｂがその暗号文Ｃを元の平文（メッセージ）Ｍに復号する場合を示している。

【００３５】

ｊ（ｊ＝１，２，・・・，Ｊ）番目のセンタ１には、各エンティティのａ，ｂ

の分割特定情報（分割ＩＤベクトル）を用いて各エンティティａ，ｂ固有の秘密鍵を生成する秘密鍵生成器１ａが備えられている。そして、各エンティティａ，ｂから登録が依頼されると、そのエンティティａ，ｂの秘密鍵（秘密ベクトル）がエンティティａ，ｂへ送付される。

【００３６】

エンティティａ側には、Ｊ個の各センタ１から送られる固有の秘密鍵をテーブル形式で格納しているメモリ１０と、これらの秘密鍵の中からエンティティｂに対応する成分を選び出す成分選出器１１と、選び出されたこれらの成分を合成してエンティティａが求めるエンティティｂとの共通鍵K_{ab}を生成する共通鍵生成器１２と、共通鍵K_{ab}を用いて平文（メッセージ）Ｍを暗号文Ｃに暗号化して通信路３０へ出力する暗号化器１３とが備えられている。

【００３７】

また、エンティティｂ側には、各センタ１から送られる固有の秘密鍵をテーブル形式で格納しているメモリ２０と、これらの秘密鍵の中からエンティティａに対応する成分を選び出す成分選出器２１と、選び出されたこれらの成分を合成してエンティティｂが求めるエンティティａとの共通鍵K_{ba}を生成する共通鍵生成器２２と、共通鍵K_{ba}を用いて通信路３０から入力した暗号文Ｃを平文（メッセージ）Ｍに復号して出力する復号器２３とが備えられている。

【００３８】

次に、このような構成の暗号通信システムにおける暗号通信の処理動作について説明する。

【００３９】

（予備処理）

各エンティティの氏名，住所などを示す特定情報であるＩＤベクトルをＬ次元２進ベクトルとし、図３に示すようにそのＩＤベクトルをブロックサイズM_1，M_2，・・・，M_J毎にＪ個のブロックに分割する。例えば、エンティティａのＩＤベクトル（ベクトルI_a）を下記（５）のように分割する。分割特定情報である各ベクトルI_{aj}（ｊ＝１，２，・・・，Ｊ）をＩＤ分割ベクトルと呼ぶ。ここで、M_j＝Ｍとすると、全てのＩＤ分割ベクトルのサイズが等しくなる。また

、M_j ＝１と設定することも可能である。なお、各エンティティの公開ＩＤベクトルはハッシュ関数により、Ｌビットに変換される。なお、以下では説明を簡単にするために、M_j ＝Ｍ（一定）とする。

【００４０】

【数３】

$$\overrightarrow{I_a} = [\overrightarrow{I_{a1}} \mid \overrightarrow{I_{a2}} \mid \cdots \mid \overrightarrow{I_{aJ}}] \quad \cdots (5)$$

【００４１】

以下、本発明の３種の例について具体的に説明する。

（第１実施の形態）

〔秘密鍵の生成・配布処理〕

ｊ番目のセンタ１は、ランダムな数を要素とする対称行列H_j （$2^M \times 2^M$）を生成する。但し、共通鍵のサイズをＳとして、上記（２）～（４）の条件を満たす。

【００４２】

また、ｊ番目のセンタ１は、Ｓビットを出力するハッシュ関数f_j （・）を生成し、秘密裏に次の（ｊ＋１）番目のセンタ１へ送付する。但し、Ｊ番目のセンタ１は、１番目のセンタ１へ送付する。

【００４３】

そして、ｊ番目のセンタ１は、エンティティａに対して、対称行列H_j より、そのエンティティａのＩＤ分割ベクトルに対応する行ベクトルを取り出し、取り出した行ベクトルの全ての成分に個人乱数$\alpha_a^{(j)}$ をＸＯＲしたものを秘密鍵ベクトルs_{aj}として生成し、それをエンティティａへ秘密裏に配布する。

【００４４】

即ち、ｍ＝０，１，２，・・・，2^M －１に対して、下記（６）を秘密鍵ベクトルs_{aj}として配布する。なお、$\alpha_a^{(j)}$ を、下記（７）のように設定する。但し、ｊ－１＝０である場合にはＪとして扱う。なお、$k_{aj,m}^{(j)}$ は、エンティティａのＩＤ分割ベクトルに対応する行ベクトルの各成分を示す。

【００４５】

【数４】

$$s_{a_j,m} = k^{(j)}_{a_j,m} \oplus \alpha^{(j)}_a \qquad \cdots(6)$$

$$\alpha^{(j)}_a = f_j(ID_a) \oplus f_{j-1}(ID_a) \qquad \cdots(7)$$

【００４６】

〔共通鍵の生成（鍵共有）〕

エンティティａは、Ｊ個の各センタから受け取った秘密ベクトルから、エンティティｂに対応する成分を取り出し、これらのＪ個の成分をＸＯＲにより合成して、エンティティｂに対する共通鍵K_{ab}を生成する。この際、エンティティａに関する全ての個人乱数$\alpha_a^{(j)}$をＸＯＲした場合、同一のハッシュ値が２度ずつＸＯＲされて０になるので、下記（８）が成立する。

【００４７】

【数５】

$$K_{ab} = \bigoplus_{j=1}^{J} s_{a_j b_j}$$

$$= \bigoplus_{j=1}^{J} \left(k^{(j)}_{a_j b_j} \oplus \alpha^{(j)}_a \right)$$

$$= \bigoplus_{j=1}^{J} k^{(j)}_{a_j b_j} \qquad \cdots(8)$$

【００４８】

エンティティｂも、エンティティａに対して共通鍵K_{ba}を同様に生成する。ここで、Ｊ個の各センタｌが有する秘密情報（行列H_j）の対称性に基づいて、両

共通鍵K_{ab}，K_{ba}は一致する。

【００４９】

この第１実施の形態では、センタの秘密が露呈しないので、安全性が高い。また、各エンティティの個人乱数を設定するような特定のセンタの存在は不要であり、Big Brother の問題を全く排除している。

【００５０】

（第２実施の形態）

〔秘密鍵の生成・配布処理〕

ｊ番目のセンタ１は、第１実施の形態と同様に、対称行列H_jを生成する。また、Ｓビットを出力する関数g_j（・）を生成して公開する。

【００５１】

そして、ｊ番目のセンタ１は、エンティティａについて、対称行列H_jより、そのエンティティａのＩＤ分割ベクトルに対応する行ベクトルを取り出し、取り出した行ベクトルの全ての成分に対して、g_j（ID_a）のビットパターンによりマスクしたものを秘密鍵ベクトルs_{aj}として生成し、それをエンティティａへ秘密裏に配布する。なお、ここでのマスク処理は、ビット毎のＡＮＤ演算である。

【００５２】

〔共通鍵の生成（鍵共有）〕

エンティティａは、Ｊ個の各センタから受け取った秘密ベクトルから、エンティティｂに対応する成分を取り出し、これらの成分に対してg_j（ID_b）を自身の秘密鍵の各成分にマスクした値を、ｊ＝１からＪまでＸＯＲにより合成して、エンティティｂに対する共通鍵K_{ab}を生成する。即ち、下記（９）が成立する。

【００５３】

【数６】

$$K_{ab} = \bigoplus_{j=1}^{J} (s_{a_j b_j} \cap g_j(ID_b))$$

$$= \bigoplus_{j=1}^{J} k^{(j)}_{a_j b_j} \cap g_j(ID_a) \cap g_j(ID_b)) \quad \cdots (9)$$

【００５４】

エンティティｂも、エンティティａに対して共通鍵K_{ba}を同様に生成する。ここで、Ｊ個の各センタ１が有する秘密情報（行列H_j）の対称性に基づいて、両共通鍵K_{ab}，K_{ba}は一致する。

【００５５】

この第２実施の形態では、配布される秘密鍵には、センタが生成した秘密情報（行列H_j）のうちの一部の情報しか含まれていない。例えば、エンティティａ，ｂのＩＤベクトルが部分的に等しい場合でも、マスクg_j（ID_a）とg_j（ID_b）とが異なるので、秘密鍵ベクトルs_{aj}とs_{bj}とは同一でない。従って、センタの秘密行列の全情報を得るためには、非常に多数のエンティティによる結託が必要であり、結託閾値を高くすることができる。

【００５６】

（第３実施の形態）

上述した第１実施の形態，第２実施の形態を融合した第３実施の形態について説明する。この第３実施の形態は、乱数置換攻撃が成立しないという特徴を有する。

【００５７】

〔秘密鍵の生成・配布処理〕

ｊ番目のセンタ１は、第１実施の形態と同様に、対称行列H_jを生成する。また、ｊ番目のセンタ１は、Ｓビットを出力するハッシュ関数f_j（・）を生成し

、秘密裏に次の（ｊ＋１）番目のセンタ１へ送付する。但し、Ｊ番目のセンタ１は、１番目のセンタ１へ送付する。また、Ｓビットを出力する関数g_j（・）を生成して公開する。

【００５８】

そして、ｊ番目のセンタ１は、エンティティａについて、対称行列H_jより、そのエンティティａのＩＤ分割ベクトルに対応する行ベクトルを取り出し、取り出した行ベクトルの全ての成分に対して、g_j（ID_a）のビットパターンによりマスクし、更に個人乱数$\alpha_a^{(j)}$をＸＯＲしたものを秘密鍵ベクトルs_{aj}として生成し、それをエンティティａへ秘密裏に配布する。なお、ここでのマスク処理は、ビット毎のＡＮＤ演算である。

【００５９】

即ち、ｍ＝０，１，２，・・・，2^M-1に対して、下記（10）を秘密鍵ベクトルs_{aj}として配布する。なお、$\alpha_a^{(j)}$，$\beta_a^{(j)}$を、下記（11），（12）のように設定する。但し、ｊ－１＝０である場合にはＪとして扱う。

【００６０】

【数７】

$$s_{a_j,m}=\left(k^{(j)}_{a_j,m}\cap\beta^{(j)}_a\right)\oplus\alpha^{(j)}_a \quad \cdots(10)$$

$$\alpha^{(j)}_a=f_j(ID_a)\oplus f_{j-1}(ID_a) \quad \cdots(11)$$

$$\beta^{(j)}_a=g_j(ID_a) \quad \cdots(12)$$

【００６１】

〔共通鍵の生成（鍵共有）〕

エンティティａは、Ｊ個の各センタから受け取った秘密ベクトルから、エンティティｂに対応する成分を取り出し、第１実施の形態と同様に、これらのＪ個の成分をＸＯＲにより合成して、下記（13）のように中間鍵K_{ab}'を生成する。こ

の際、エンティティａに関する同一のハッシュ値が２度ずつＸＯＲされて０になることは、第１実施の形態と同様である。

【００６２】

【数８】

$$K_{ab}' = \bigoplus_{j=1}^{J} s_{a_j b_j} \quad \cdots(13)$$

【００６３】

次に、中間鍵K_{ab}'から、互いのマスク値を考慮して、有効なビット成分を抜き出して、下記（14）のように、エンティティｂに対する共通鍵K_{ab}を生成する。但し、バーｘはｘのビット毎の否定演算を表す。

【００６４】

【数９】

$$K_{ab} = K_{ab}' \cap \bigcap_{j=1}^{J} \overline{\beta_a^{(j)} \oplus \beta_b^{(j)}} \quad \cdots(14)$$

【００６５】

エンティティｂも、エンティティａに対して共通鍵K_{ba}を同様に生成する。ここで、Ｊ個の各センタ１が有する秘密情報（行列H_j）の対称性に基づいて、両共通鍵K_{ab}，K_{ba}は一致する。

【００６６】

この第３実施の形態における安全性について説明する。第３実施の形態では、各ブロックに個人乱数がＸＯＲされているので、第２実施の形態のようにブロック毎にセンタの秘密行列の部分情報が漏れることはない。また、特定のエンティティを攻撃するために乱数置換攻撃を適用した場合にあっても、マスク処理の影

響によって、この攻撃は成立しない。

【００６７】

第３実施の形態では第２実施の形態と同様、結託閾値を向上させるためにマスク処理という手法を用いている。よって、安全性は向上するが、Ｊを大きくした場合、最終的に鍵共有に使用可能な有効ビットの数が急激に減少することが考えられる。そこで、このことを解消するために、次の（ａ），（ｂ）のような対策が可能である。

【００６８】

（ａ）暗号通信システム全体で共通の関数ｇ（・）を設定し、各センタが設定しているマスク値を求める関数をg_j（・）＝ｇ（・）とする。

（ｂ）暗号通信システム全体で共通の関数ｇ（・）を設定し、前半Ｊ／２のセンタはg_j（・）＝ｇ（・）とし、後半Ｊ／２のセンタはg_j（・）＝バーｇ（・）とする。

【００６９】

（ａ）の対策では、マスク部分が減少するようなことはないが、０でマスクされていた部分は鍵共有時に０となるので、関数ｇ（・）が０と１とを一様に出力すると仮定した場合、鍵共有に使用される有効部分は全体の１／４程度となる。

【００７０】

（ｂ）の対策では、下記（15）が成立するので、上記（14）のマスク部分が減少することはない。しかしながら前半のセンタにおいて０でマスクされていたために鍵共有時に０となる部分が、後半のセンタにおいては１でマスクされているために鍵共有時に有効となる。このため、関数ｇ（・）が０と１とを一様に出力すると仮定した場合、鍵共有に使用される有効部分は全体の１／２程度となる。

【００７１】

【数１０】

$$g(ID_a) \oplus g(ID_b) = \overline{g(ID_a) \oplus g(ID_b)} \quad \cdots(15)$$

【００７２】

図４は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、上述した第１実施の形態における各エンティティ固有の秘密鍵の生成処理、第２実施の形態における各エンティティ固有の秘密鍵の生成処理または第３実施の形態における各エンティティ固有の秘密鍵の生成処理を含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ４０は、各センタ側に設けられている。

【００７３】

図４において、コンピュータ４０とオンライン接続する記録媒体４１は、コンピュータ４０の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体４１には前述の如きプログラム４１ａが記録されている。記録媒体４１から読み出されたプログラム４１ａがコンピュータ４０を制御することにより、各センタにおいて各エンティティ固有の秘密鍵を生成する。

【００７４】

コンピュータ４０の内部に設けられた記録媒体４２は、内蔵設置される例えばハードディスクドライブまたはＲＯＭなどを用いてなり、記録媒体４２には前述の如きプログラム４２ａが記録されている。記録媒体４２から読み出されたプログラム４２ａがコンピュータ４０を制御することにより、各センタにおいて各エンティティ固有の秘密鍵を生成する。

【００７５】

コンピュータ４０に設けられたディスクドライブ４０ａに装填して使用される記録媒体４３は、運搬可能な例えば光磁気ディスク，ＣＤ－ＲＯＭまたはフレキ

シブルディスクなどを用いてなり、記録媒体４３には前述の如きプログラム４３ａが記録されている。記録媒体４３から読み出されたプログラム４３ａがコンピュータ４０を制御することにより、各センタにおいて各エンティティ固有の秘密鍵を生成する。

【００７６】

【発明の効果】

本発明では、エンティティの各分割特定情報に応じて対称行列の一部の成分を取り出し、取り出した成分に各エンティティ固有の乱数を合成して、各エンティティ固有の秘密鍵を生成するようにしたので、個人乱数を加えることによってセンタの秘密が露呈されず、安全性を向上することができる。

【００７７】

また、自身で生成したハッシュ関数と他のセンタで生成されたハッシュ関数とを用いて、取り出した成分に合成すべき乱数を生成するようにしたので、全てのセンタが対等となり、ある特定のセンタがBig Brother となることを防止できる。

【００７８】

また、エンティティの各分割特定情報に応じて対称行列の一部の成分を取り出し、その分割特定情報に基づいて各センタ固有のマスクパターンを生成し、取り出した成分をそのマスクパターンでマスクして、各エンティティ固有の秘密鍵を生成するようにしたので、両エンティティにおいて分割特定情報が同じであっても、そのマスクパターンは異なるため、結託攻撃に強くなり、結託閾値を高くすることができる。

【００７９】

また、以上のような個人乱数付加とマスク処理とを融合させて各エンティティ固有の秘密鍵を生成するようにしたので、乱数置換攻撃を全く受けない暗号方式を提供できる。更に、本発明では、共通鍵を生成する際に各センタからの成分をＸＯＲ合成しており、桁上がりの問題を解消できる。

【００８０】

（付記）

なお、以上の説明に対して更に以下の項を開示する。

（１）　請求項２に記載の秘密鍵生成方法であって、Ｊ個のセンタが存在し、ｊ番目（ｊ＝１，２，…，Ｊ）のセンタは自身が生成した前記ハッシュ関数を（ｊ＋１）番目（ｊ＝Ｊの場合は１番目）のセンタへ送付し、（ｊ＋１）番目（ｊ＝Ｊの場合は１番目）のセンタにて、自身が生成したハッシュ関数と送付されたｊ番目のセンタのハッシュ関数とに基づいて、自身での前記乱数を生成する秘密鍵生成方法。

（２）　複数のセンタの夫々にて、エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎の秘密の対称行列とを用いて、前記エンティティ固有の秘密鍵を生成する方法において、前記各分割特定情報に応じて前記対称行列の一部の成分を取り出し、前記各分割特定情報に応じて各センタ固有のマスクパターンを生成し、取り出した成分を前記マスクパターンでマスクし、そのマスク結果に前記エンティティ固有の乱数を合成することにより、前記エンティティ固有の秘密鍵を生成する秘密鍵生成方法。

（３）　第（２）項に記載の秘密鍵生成方法であって、一のセンタ自身で生成したハッシュ関数と他のセンタで生成されたハッシュ関数とに基づいて、前記一のセンタでの前記乱数を生成する秘密鍵生成方法。

（４）　第（３）項に記載の秘密鍵生成方法であって、Ｊ個のセンタが存在し、ｊ番目（ｊ＝１，２，…，Ｊ）のセンタは自身が生成した前記ハッシュ関数を（ｊ＋１）番目（ｊ＝Ｊの場合は１番目）のセンタへ送付し、（ｊ＋１）番目（ｊ＝Ｊの場合は１番目）のセンタにて、自身が生成したハッシュ関数と送付されたｊ番目のセンタのハッシュ関数とに基づいて、自身での前記乱数を生成する秘密鍵生成方法。

（５）　複数のセンタの夫々にて、各エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ毎の秘密の対称行列とを用いて、各エンティティ固有の秘密鍵を生成し、この秘密鍵に含まれている暗号文の送信先である相手のエンティティに対応する成分を使用して生成した共通鍵を用いて平文を暗号文に暗号化する暗号化方法において、請求項１～３，第（１）項～第（４）項の何れかに記載の秘密鍵生成方法によって生成された各エンティティ固有の秘密

鍵を使用する暗号化方法。

（６）　エンティティ間の暗号通信にあって、平文から暗号文への暗号化処理及び暗号文から平文への復号処理に用いる共通鍵を生成する方法において、一方のエンティティの特定情報を複数のブロックに分割した各分割特定情報を用いて生成された前記一方のエンティティ固有の各秘密鍵に含まれている通信相手の他方のエンティティに対応する成分を夫々取り出し、取り出した成分をＸＯＲ合成して前記共通鍵を生成する共通鍵生成方法。

（７）　エンティティ間の暗号通信にあって、平文から暗号文への暗号化処理及び暗号文から平文への復号処理に用いる共通鍵を生成する方法において、請求項１～３，第（１）項～第（４）項の何れかに記載の秘密鍵生成方法によって生成された一方のエンティティ固有の各秘密鍵に含まれている通信相手の他方のエンティティに対応する成分を夫々取り出し、取り出した成分をＸＯＲ合成して前記共通鍵を生成する共通鍵生成方法。

（８）　センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行うこととし、前記センタが複数設けられており、その複数のセンタ夫々は、各エンティティ固有の秘密鍵を生成するようにした暗号通信方法において、請求項１～３，第（１）項～第（４）項の何れかに記載の秘密鍵生成方法によって各エンティティ固有の秘密鍵を生成する暗号通信方法。

（９）　センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行うこととし、前記セン

タが複数設けられており、その複数のセンタ夫々は、各エンティティ固有の秘密鍵を生成し、各エンティティは、自身固有の複数の秘密鍵に含まれている相手のエンティティに対応する成分を使用して前記共通鍵を生成するようにした暗号通信方法において、請求項１～３，第（１）項～第（４）項の何れかに記載の秘密鍵生成方法によって一方のエンティティ固有の秘密鍵を生成し、生成された一方のエンティティ固有の各秘密鍵に含まれている通信相手の他方のエンティティに対応する成分を夫々取り出し、取り出した成分をＸＯＲ合成して前記共通鍵を生成する暗号通信方法。

（１０）　送信すべき情報である平文を暗号文に暗号化する暗号化処理、及び、送信された暗号文を元の平文に復号する復号処理を、複数のエンティティ間で相互に行うこととし、各エンティティ固有の秘密鍵を生成して各エンティティへ送付する複数のセンタと、該センタから送付された自身固有の複数の秘密鍵に含まれている通信対象のエンティティに対応する成分を使用して、前記暗号化処理及び復号処理に用いる共通鍵を生成する複数のエンティティとを有する暗号通信システムにおいて、請求項１～３，第（１）項～第（４）項の何れかに記載の秘密鍵生成方法によって各エンティティ固有の秘密鍵を生成するようにした暗号通信システム。

（１１）　コンピュータに、エンティティの特定情報を複数のブロックに分割した各分割特定情報と秘密の対称行列とを用いて、前記エンティティ固有の秘密鍵を生成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、前記各分割特定情報に応じて前記対称行列の一部の成分を取り出すことをコンピュータに実行させるプログラムコード手段と、取り出した成分に前記エンティティ固有の乱数を合成することにより、前記エンティティ固有の秘密鍵を生成することをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されている記録媒体。

（１２）　コンピュータに、エンティティの特定情報を複数のブロックに分割した各分割特定情報と秘密の対称行列とを用いて、前記エンティティ固有の秘密鍵を生成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、前記各分割特定情報に応じて前記対称行列の一部の成分

を取り出すことをコンピュータに実行させるプログラムコード手段と、前記各分割特定情報に応じてマスクパターンを生成することをコンピュータに実行させるプログラムコード手段と、取り出した成分を前記マスクパターンでマスクすることにより、前記エンティティ固有の秘密鍵を生成することをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されている記録媒体。

【図面の簡単な説明】

【図１】

本発明の暗号通信システムの構成を示す模式図である。

【図２】

２人のエンティティ間における情報の通信状態を示す模式図である。

【図３】

エンティティのＩＤベクトルの分割例を示す模式図である。

【図４】

記録媒体の実施の形態の構成を示す図である。

【図５】

ＩＤ－ＮＩＫＳのシステムの原理構成図である。

【符号の説明】

１　センタ

１ａ　秘密鍵生成器

１０，２０　メモリ

１１，２１　成分選出器

１２，２２　共通鍵生成器

１３　暗号化器

２３　復号器

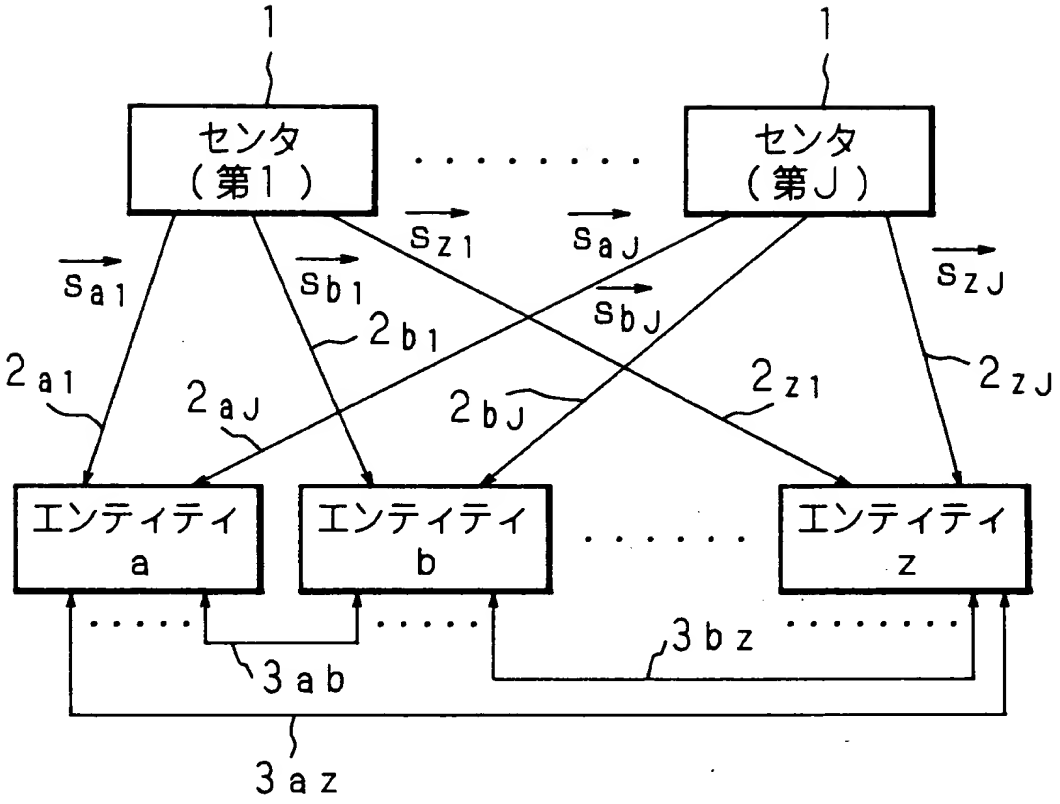
３０　通信路

４０　コンピュータ

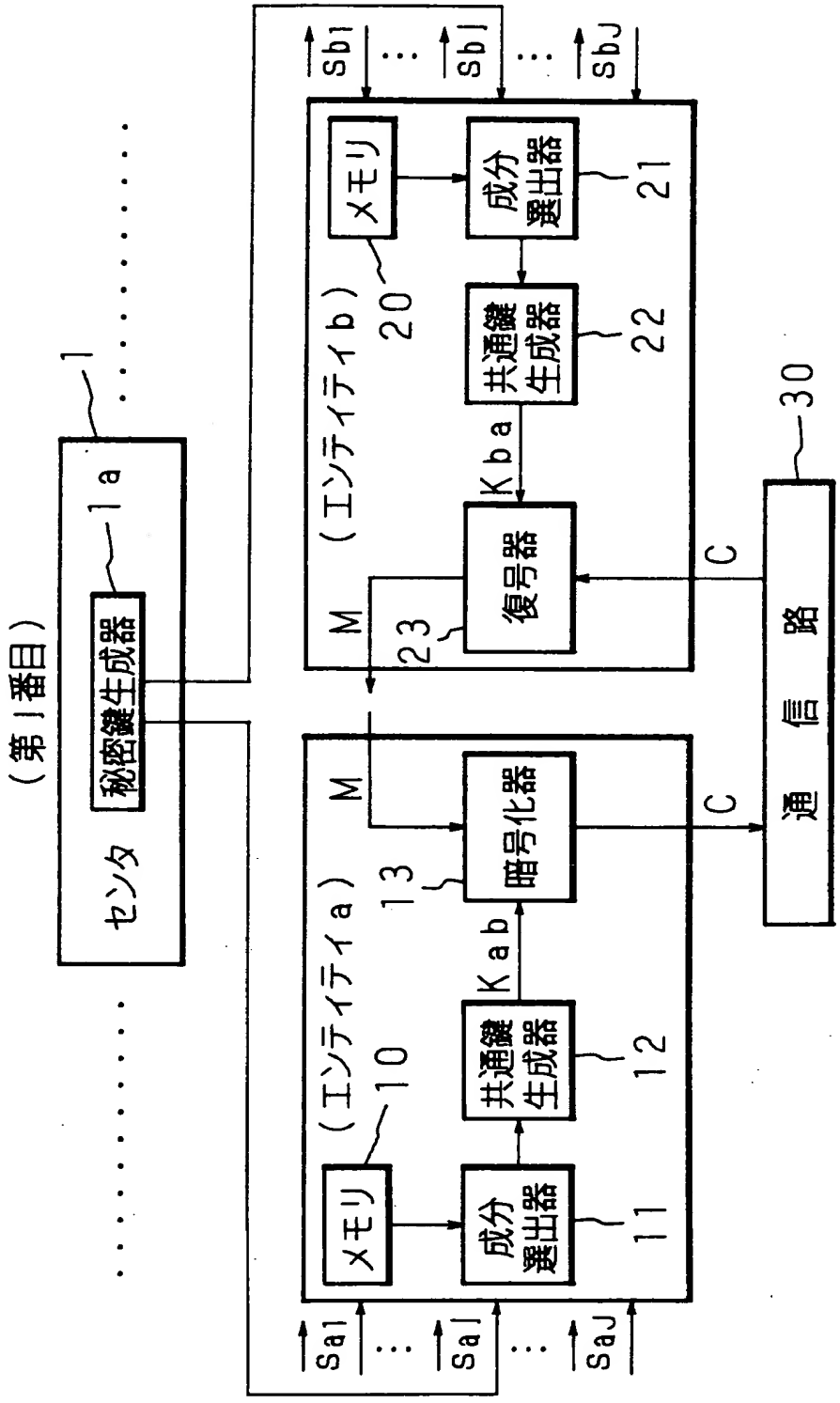
４１，４２，４３　記録媒体

【書類名】　　図面

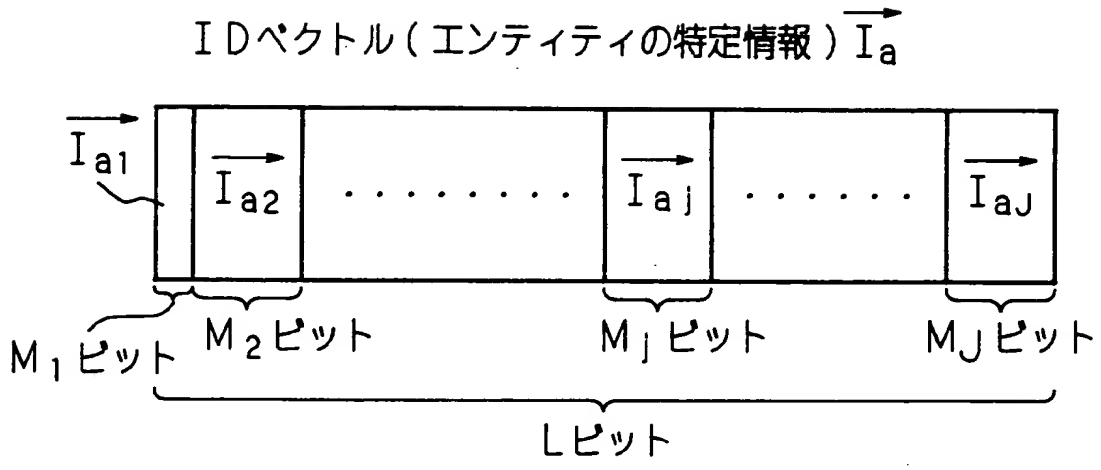
【図１】


1
1
センタ
（第１）
センタ
（第Ｊ）
Sz1
SaJ
Sa1
Sb1
SbJ
SzJ
2b1
2a1
2aJ
2bJ
2z1
2zJ
エンティティ
a
エンティティ
b
エンティティ
z
3ab
3bz
3az

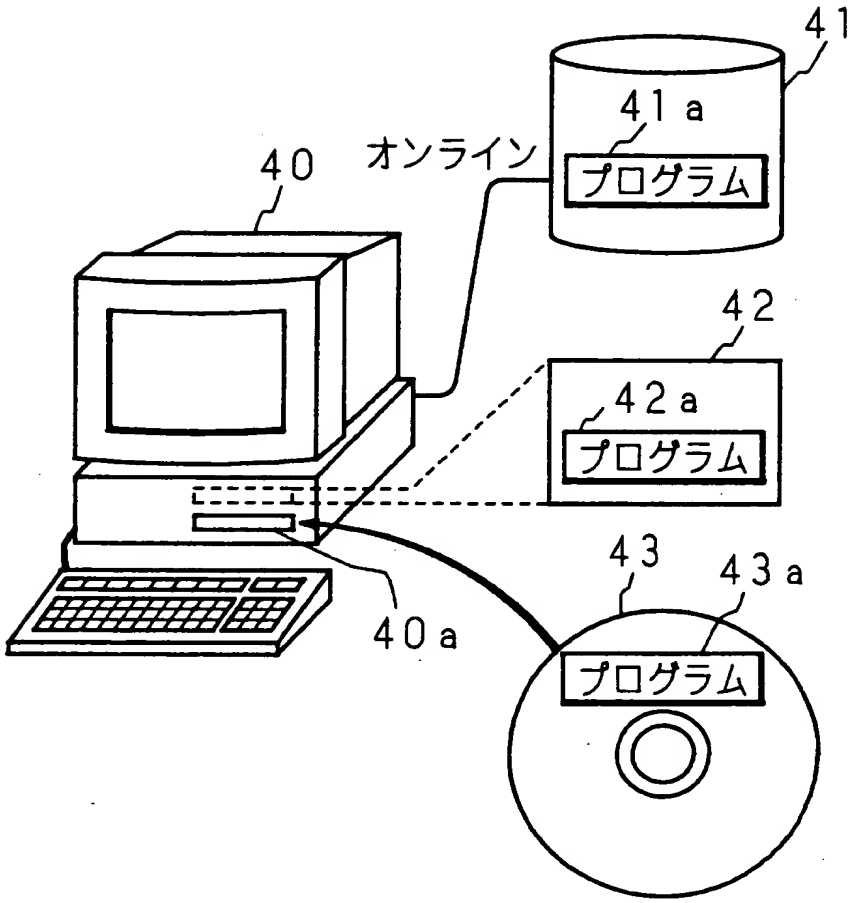
【図２】


（第１番目）
センタ
秘密鍵生成器
1a
1
Sa1
Sa1
SaJ
（エンティティａ）
10
メモリ
成分選出器
11
共通鍵生成器
12
Kab
暗号化器
13
M
C
（エンティティｂ）
20
メモリ
成分選出器
21
共通鍵生成器
22
Kba
復号器
23
M
C
Sb1
Sb1
SbJ
通信路
30

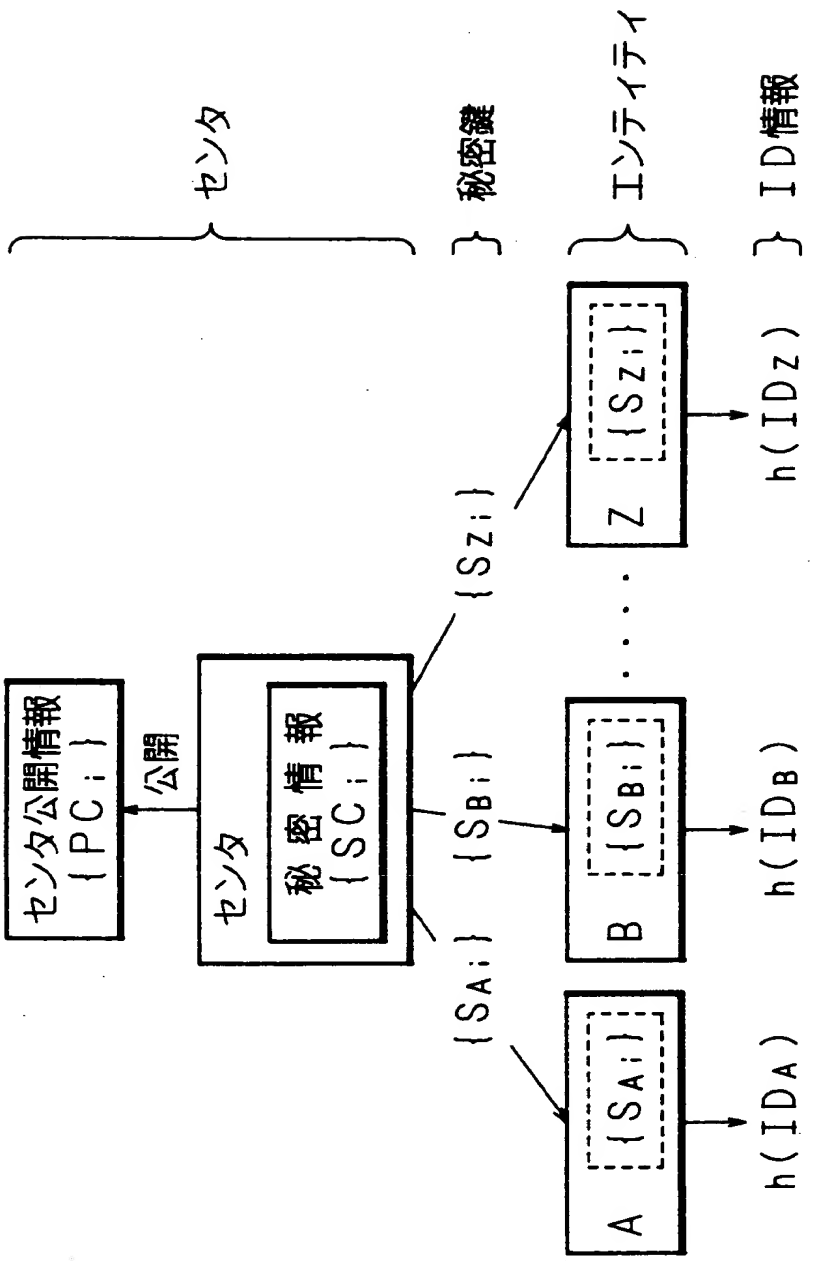
【図３】


ＩＤベクトル（エンティティの特定情報）$\overrightarrow{I_a}$
$\overrightarrow{I_{a1}}$
$\overrightarrow{I_{a2}}$
$\overrightarrow{I_{aj}}$
$\overrightarrow{I_{aJ}}$
M1ビット
M2ビット
Mjビット
MJビット
Lビット

【図４】



【図５】


センタ
秘密鍵
エンティティ
ID情報
センタ公開情報
{PCi}
公開
センタ
秘密情報
{SCi}
{SZi}
{SBi}
{SAi}
Z
{SZi}
B
{SBi}
A
{SAi}
h(IDz)
h(IDB)
h(IDA)

【書類名】　　要約書

【要約】

【課題】　エンティティ間で高速に鍵共有を行え、しかも安全性が高いＩＤ－ＮＩＫＳによる暗号通信システムを提供する。

【解決手段】　各エンティティの特定情報を複数のブロックに分割した各分割特定情報と各センタ１毎の秘密の対称行列とを用いて、各エンティティ固有の秘密鍵を生成する際に、各分割特定情報に応じてその対称行列の一部の成分を取り出し、取り出した成分に各エンティティ固有の乱数を合成して、各エンティティ固有の秘密鍵を生成する。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－０１６３５４
受付番号	５００００７３７３３
書類名	特許願
担当官	坏　政光　　８８４４
作成日	平成１２年　５月２２日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 000006297
- 【住所又は居所】 京都府京都市南区吉祥院南落合町３番地
- 【氏名又は名称】 村田機械株式会社

【特許出願人】
- 【識別番号】 597008636
- 【住所又は居所】 大阪府箕面市粟生外院４丁目１５番３号
- 【氏名又は名称】 笠原　正雄

【特許出願人】
- 【識別番号】 598159964
- 【住所又は居所】 東京都渋谷区神宮前四丁目２番１９号
- 【氏名又は名称】 辻井　重男

【復代理人】
- 【識別番号】 100114557
- 【住所又は居所】 大阪府大阪市中央区釣鐘町二丁目４番３号　河野特許事務所
- 【氏名又は名称】 河野　英仁

【代理人】 申請人
- 【識別番号】 100078868
- 【住所又は居所】 大阪府大阪市中央区釣鐘町二丁目４番３号　河野特許事務所
- 【氏名又は名称】 河野　登夫

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００６２９７〕

１．変更年月日　　１９９０年　８月　７日
［変更理由］　新規登録
住　所　京都府京都市南区吉祥院南落合町３番地
氏　名　村田機械株式会社

出　願　人　履　歴　情　報

識別番号　　〔５９７００８６３６〕

１．変更年月日　　１９９７年　１月２１日
［変更理由］　新規登録
住　所　　大阪府箕面市粟生外院４丁目１５番３号
氏　名　　笠原　正雄

出　願　人　履　歴　情　報

識別番号　　〔５９８１５９９６４〕

１．変更年月日　　１９９８年１１月１９日
［変更理由］　新規登録
住　所　東京都渋谷区神宮前四丁目２番１９号
氏　名　辻井　重男